



Donanım Güvenliđi

Yan Kanal Saldırıları

Mustafa Şirin

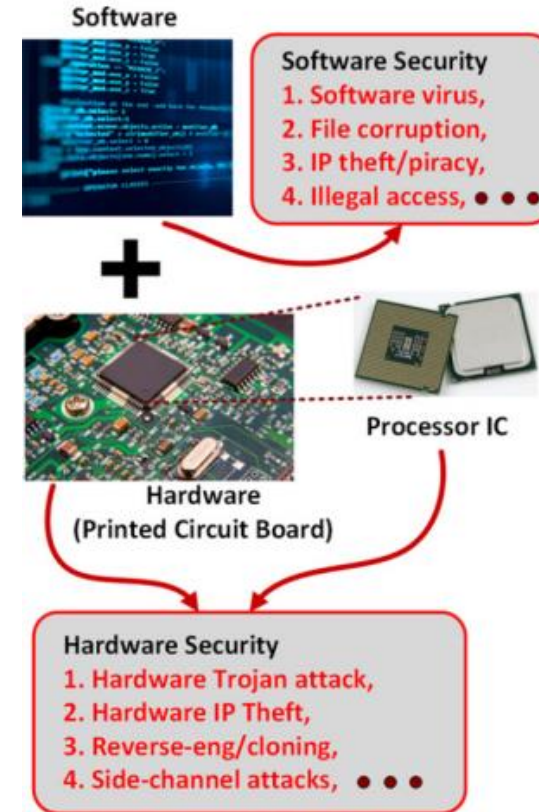
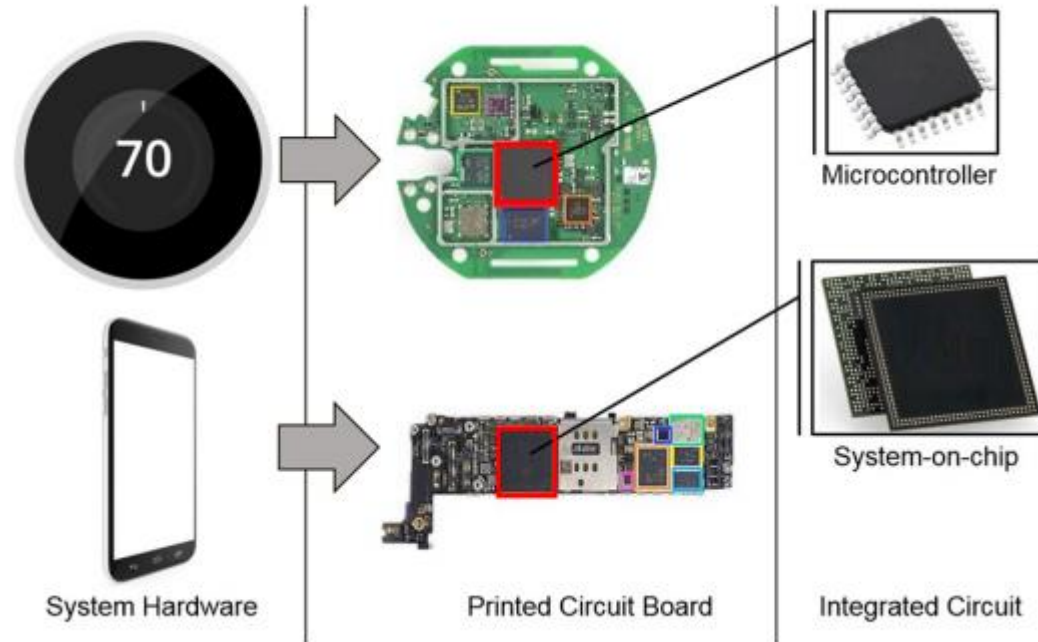
Donanım Siber Güvenlik Test Uzmanı



Program

- Donanım Güvenliği
- Donanım Güvenliği Testleri
- Kriptografi
- Yan Kanal Saldırıları
- Yan Kanal Saldırıları - LAB
 - Sinyal Analizi
 - Zamanlama Saldırısı ile Parola Elde Etme
 - Basit Güç Analizi ile RSA Anahtarı Elde Etme

Donanım Güvenliği





donanım güvenliği



Tümü

Alışveriş

Haberler

Görseller

Videolar

Daha fazla

Ayarlar

Araçlar

Yaklaşık 48.800.000 sonuç bulundu (0,42 saniye)

www.bilisimonline.net > Kategori > donanim-guvenlik ▾

Donanım Güvenliği |

Sistem odası **güvenlik**, iklimlendirme, yangın söndürme sistemleri, yedeklilik, enerji vb. Veri Merkezi (Datacenter)... Bilişim ve teknoloji alanında yaşanan hızlı ...

answers.microsoft.com > tr-tr > protect > forum > all ▾

Windows Güvenliği standart donanım güvenliği desteklenmiyor.

15 May 2020 - Windows defender cihaz güvenliği kısmında, 'standart **donanım güvenliği** desteklenmiyor' ibaresi yer almakta. Bu ne anlama geliyor cihaz ...

www.researchgate.net > publication > 279659878_TURKI...

türkiye'de yazılım/donanım ve sistem güvenliği değerlendirme ...

TÜRKİYE'DE YAZILIM/**DONANIM** VE SİSTEM **GÜVENLİĞİ** DEĞERLENDİRME ÇALIŞMALARI.
Conference Paper (PDF Available) · May 2008 with 287 Reads.

www.omeryildiz.org > genel > donanimsal-guvenlik-m... ▾

Donanım(sal) Güvenlik Modülü Nedir? Nasıl seçilmelidir ...

11 Mar 2019 - Thales N-HSM ürünü. HSM yani Hardware Security Module güzel Türkçemize “**Donanım Güvenlik Modülü**” veva “**Donanımsal Güvenlik Modülü**” ...



hardware security



Tümü

Haberler

Görseller

Alışveriş

Videolar

Daha fazla

Ayarlar

Araçlar

Yaklaşık 1.530.000.000 sonuç bulundu (0,54 saniye)

Yaklaşık 1.530.000.000 sonuç bulundu (0,54 saniye)

Hardware security is vulnerability protection that comes in the form of a physical device rather than software that is installed on the **hardware** of a computer system. Content Continues Below.

searchitoperations.techtarget.com > definition > hardware-...

[What is hardware security? - Definition from WhatIs.com](#)

Öne Çıkan Snippet'ler Hakkında

Geri bildirim

en.wikipedia.org > wiki > Har... > [Bu sayfanın çevirisini yap](#)

[Hardware security - Wikipedia](#)

Hardware security as a discipline originated out of cryptographic engineering and involves hardware design, access control, secure multi-party computation, ...

www.sciencedirect.com > topics - [Bu sayfanın çevirisini yap](#)

[Hardware Security - an overview | ScienceDirect Topics](#)

In this chapter, common **hardware security** primitives and designs for countermeasures against various threats, and vulnerabilities are discussed. First, the device- ...

www.researchgate.net > 2837... > [Bu sayfanın çevirisini yap](#)

[\(PDF\) Introduction to Hardware Security - ResearchGate](#)

PDF | Hardware security has become a hot topic recently with more and more researchers from related research domains joining this area. However, the... | Find ...

bilgem.tubitak.gov.tr > içerik > [Bu sayfanın çevirisini yap](#)

[Network HSM / Network Hardware Security Module ...](#)

Network HSM / Network Hardware Security Module. "A" operations such as signature, verification, encryption etc. over a network in a secure and fast way.

www.intel.com.tr > www > ha... - [Bu sayfanın çevirisini yap](#)

[Hardware-Enabled Security - Intel](#)

Enabling Innovation with Security at the Core. Cyber-attacks are moving down the computing stack, traversing from software to hardware, threatening devices in ...

www.quora.com > What-is-ha... - [Bu sayfanın çevirisini yap](#)

[What is hardware security? - Quora](#)

Hardware security



İngilizceden çevrilmiştir - Şifreleme mühendisliğinden kaynaklanan bir disiplin olarak donanım güvenliği ve donanım tasarımı, erişim kontrolü, güvenli çok taraflı hesaplama, güvenli anahtar depolama, kod özgünlüğünü sağlama, ürünü oluşturan tedarik zincirinin diğer şeylerin yanı sıra güvenli olmasını sağlayan önlemler içerir.

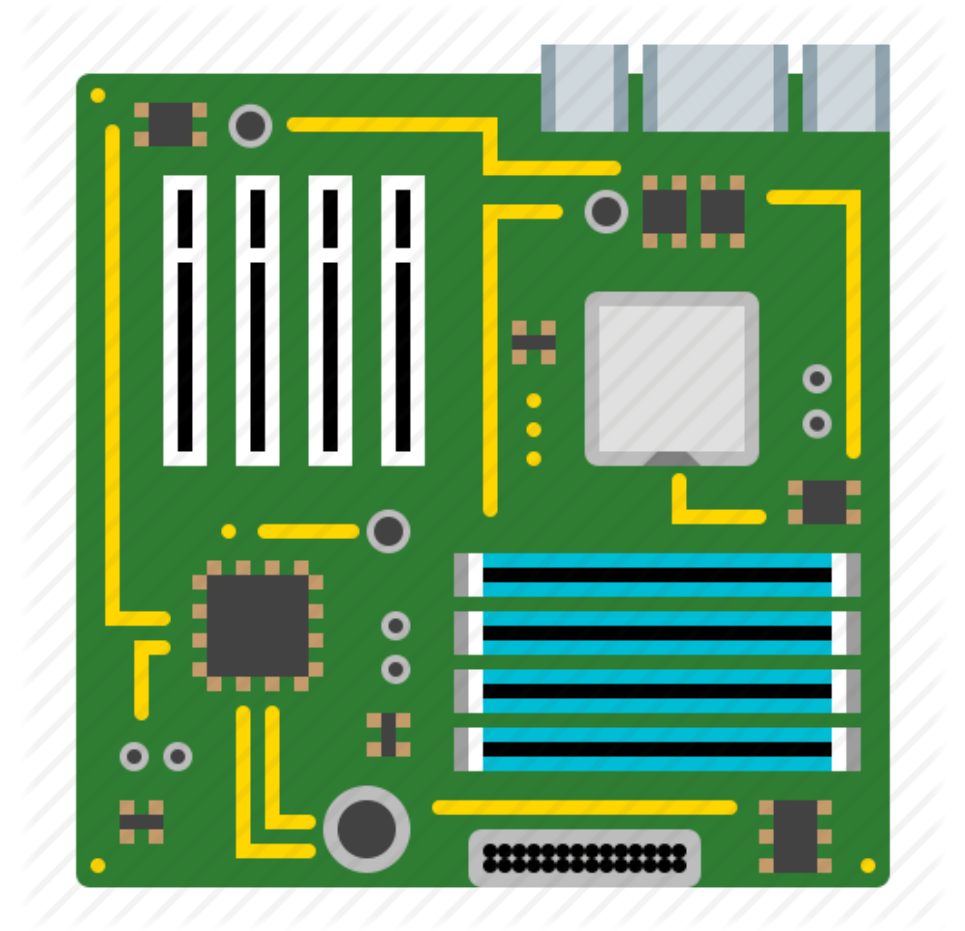
[Wikipedia \(İngilizce\)](#)

[Orijinal açıklamayı göster](#)

Geri Bildirim

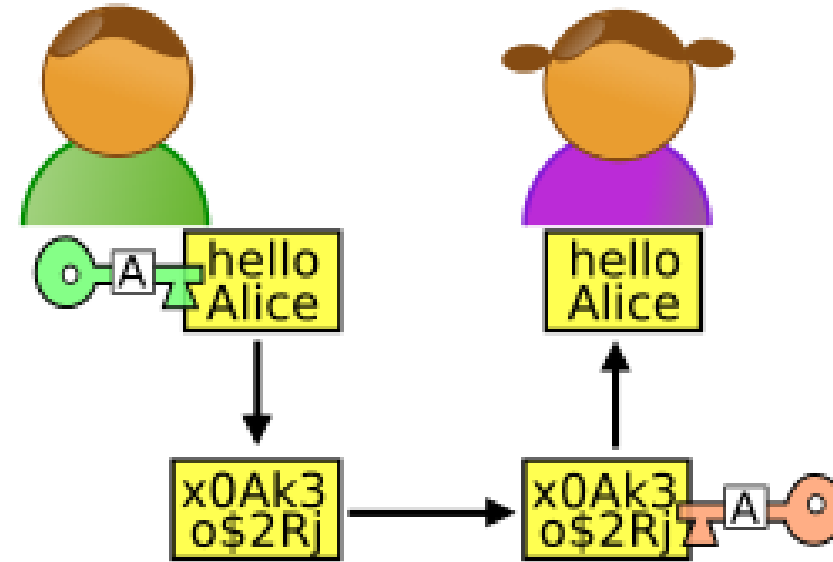
Donanım Güvenliđi Testleri

- Tersine Mühendislik Saldırıları
- Hardware Trojan
- Yan Kanal Saldırıları
- Fault Injection Saldırıları
- Fiziksel Arayüz Saldırıları
- Bus Snooping



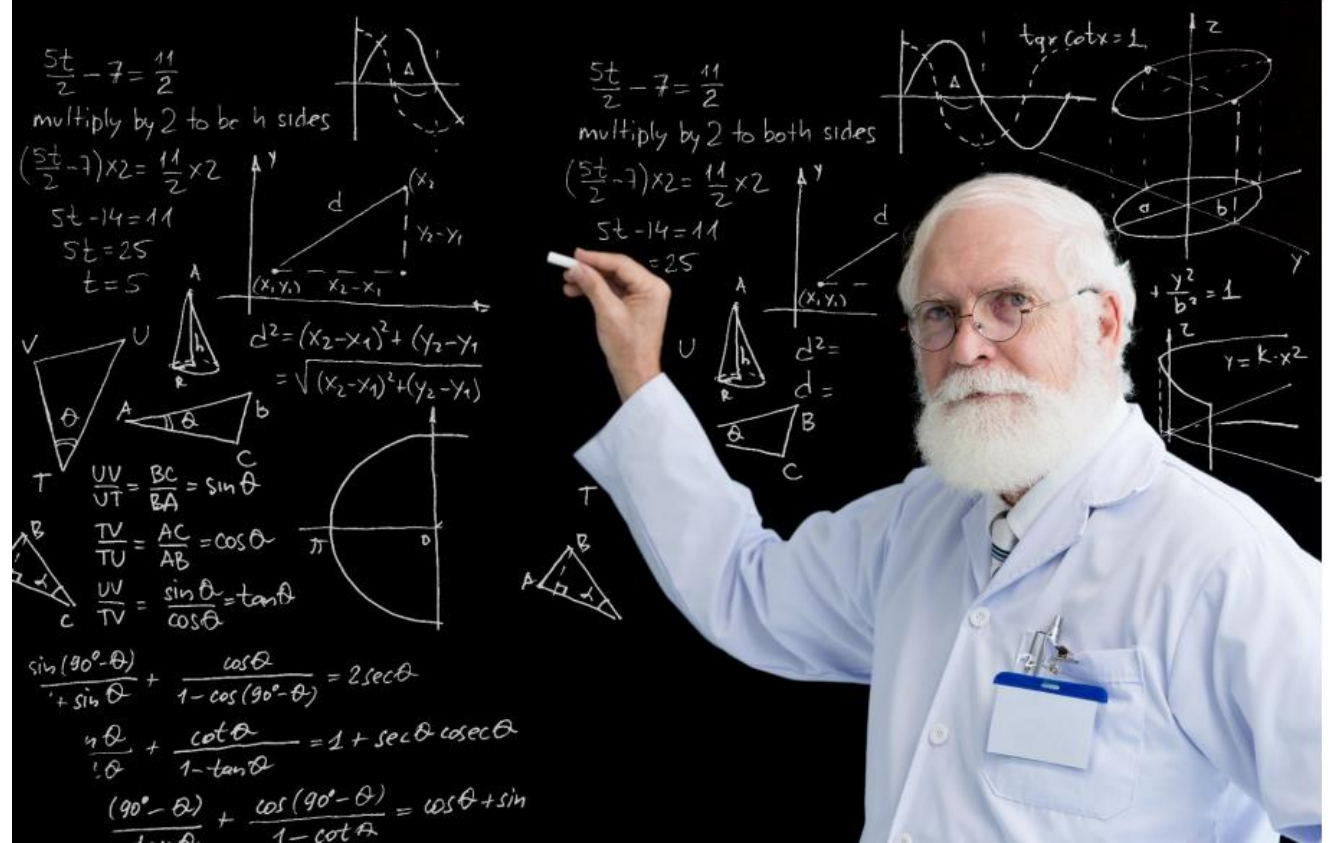
Kriptografi

- Bilgi Güvenliği
- Simetrik – Asimetrik
- Kriptanaliz
- Şifreleme Saldırıları



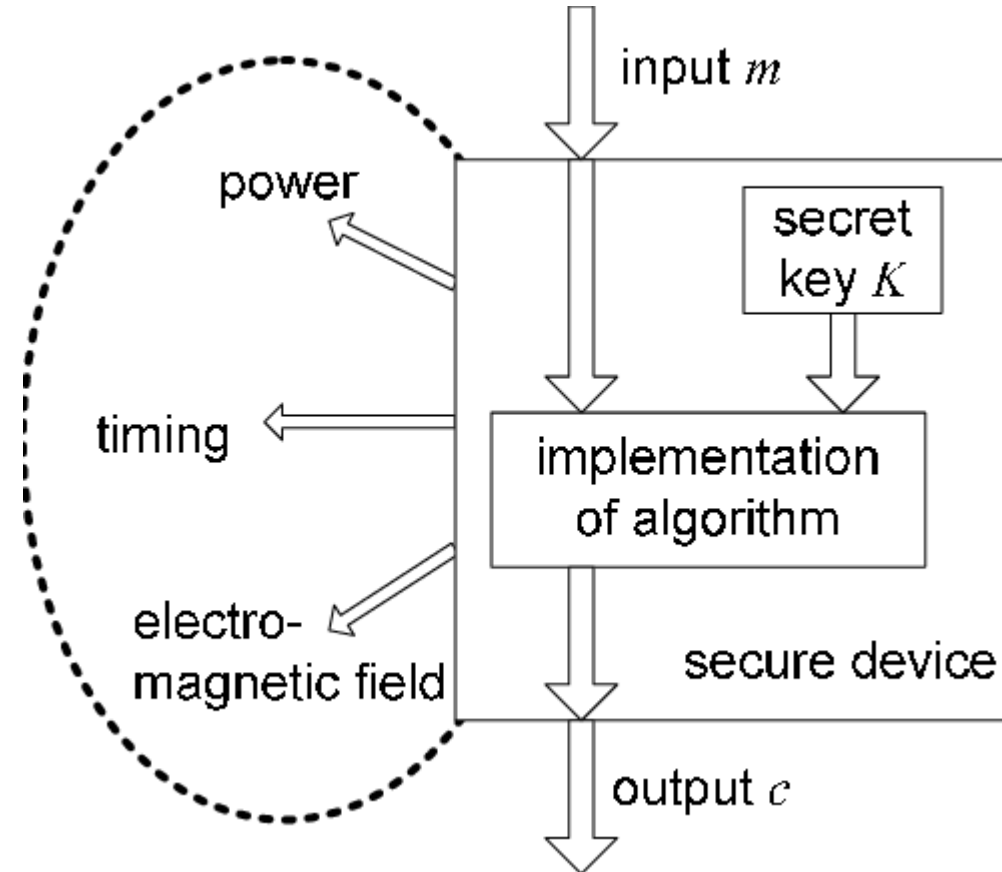
Kriptografi

- Bilgi Güvenliği
- Simetrik – Asimetrik
- Kriptanaliz
- Şifreleme Saldırıları



Yan Kanal Saldırıları

- Yan Kanal?
- Zamanlama Analizi
- Güç Analizi
- Elektromanyetik Analiz
- Ses Analizi



Yan Kanal Saldırıları

- Yan Kanal?
- Zamanlama Analizi
- Güç Analizi
- Elektromanyetik Analiz
- Ses Analizi

Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

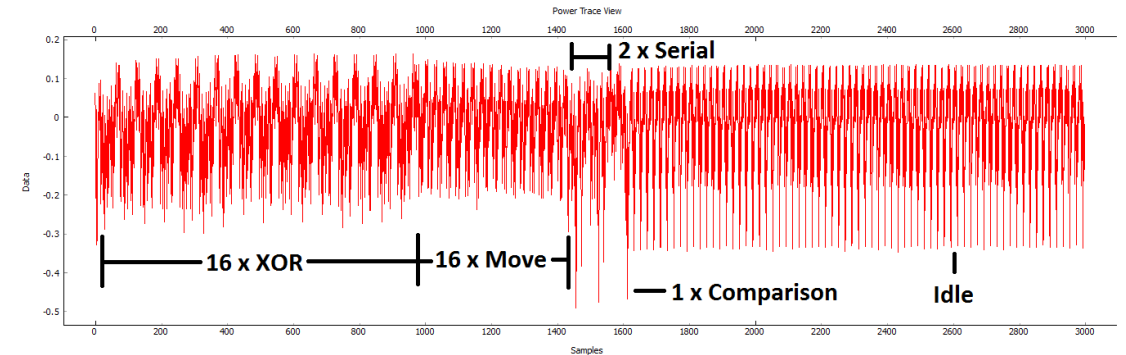
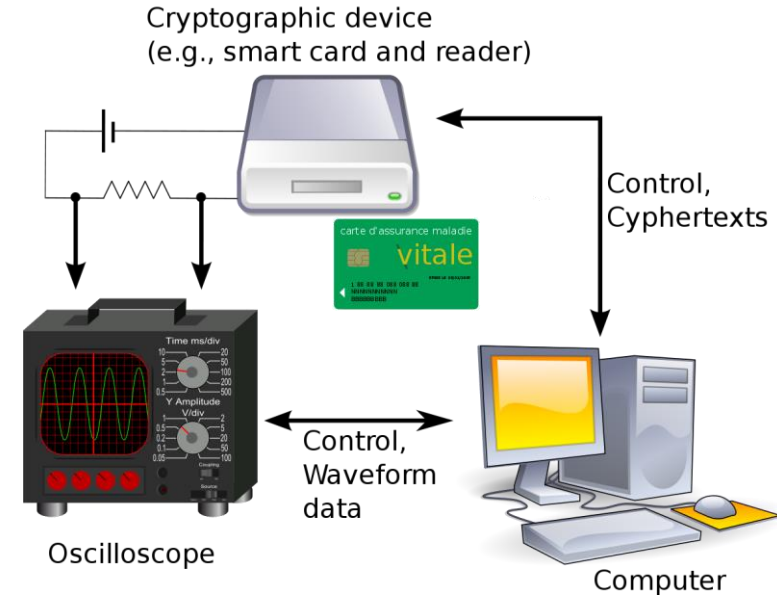
Paul C. Kocher

Cryptography Consultant
P.O. Box 8243, Stanford, CA 94309, USA.
E-mail: pck@cryptography.com.

Abstract. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems.

Yan Kanal Saldırıları

- Yan Kanal?
- Zamanlama Analizi
- Güç Analizi
- Elektromanyetik Analiz
- Ses Analizi



Yan Kanal Saldırıları

- Yan Kanal?
- Zamanlama Analizi
- Güç Analizi
- Elektromanyetik Analiz
- Ses Analizi

Differential Power Analysis

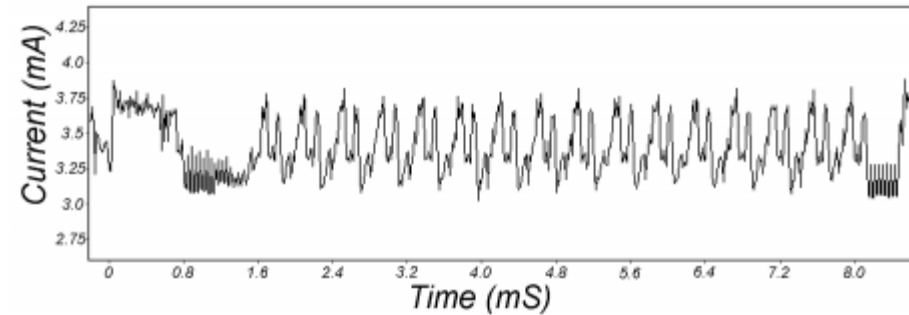
Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
870 Market Street, Suite 1088
San Francisco, CA 94102, USA.

<http://www.cryptography.com>

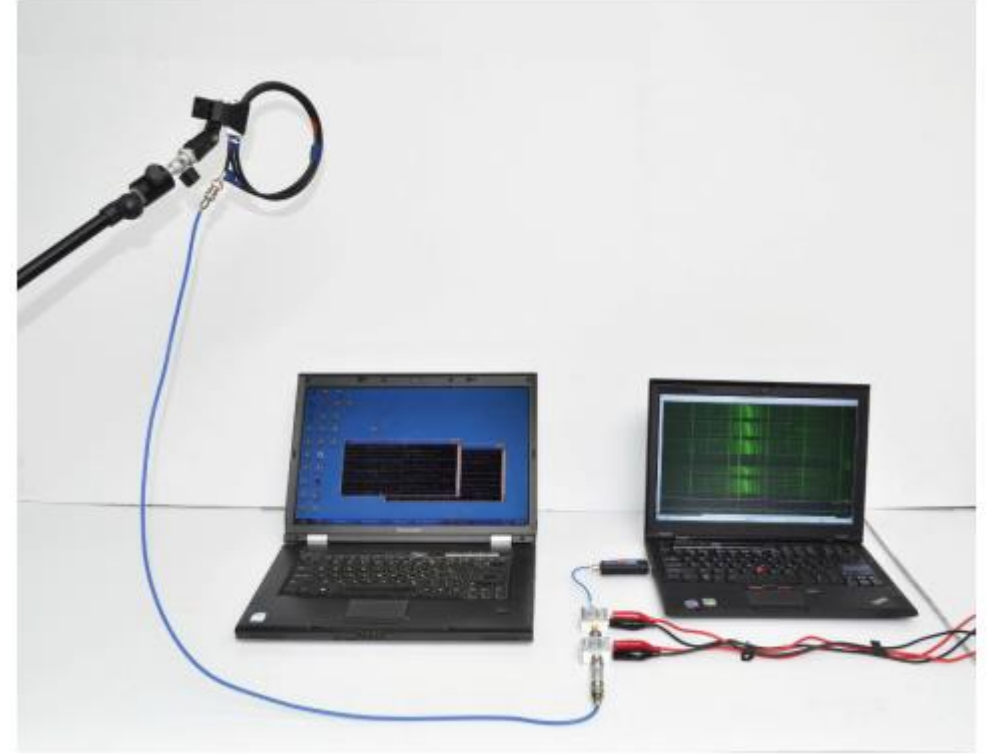
E-mail: {paul,josh,ben}@cryptography.com.

Abstract. Cryptosystem designers frequently assume that secrets will be manipulated in closed reliable computing environments. Unfortun-



Yan Kanal Saldırıları

- Yan Kanal?
- Zamanlama Analizi
- Güç Analizi
- Elektromanyetik Analiz
- Ses Analizi



Yan Kanal Saldırıları

- Yan Kanal?
- Zamanlama Analizi
- Güç Analizi
- Elektromanyetik Analiz
- Ses Analizi



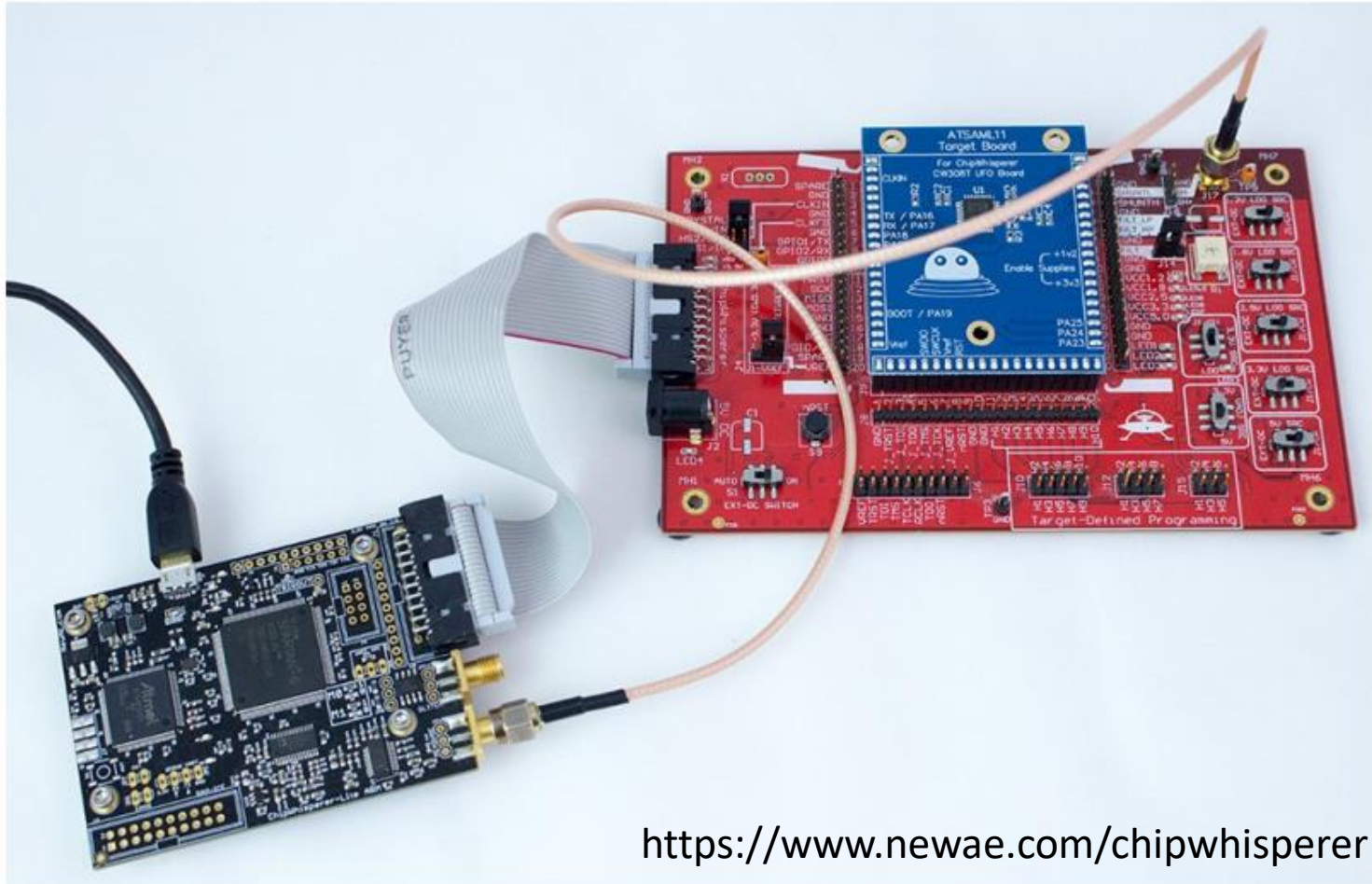
A team of researchers - including Adi Shamir, one of the trio of researchers that came up with the RSA encryption algorithm - have confirmed a theory they developed a decade ago, namely that it is possible to identify the encryption key of an 4,096 RSA encryption key from the sound that the hard drive makes when encrypting the data on the disk surface.



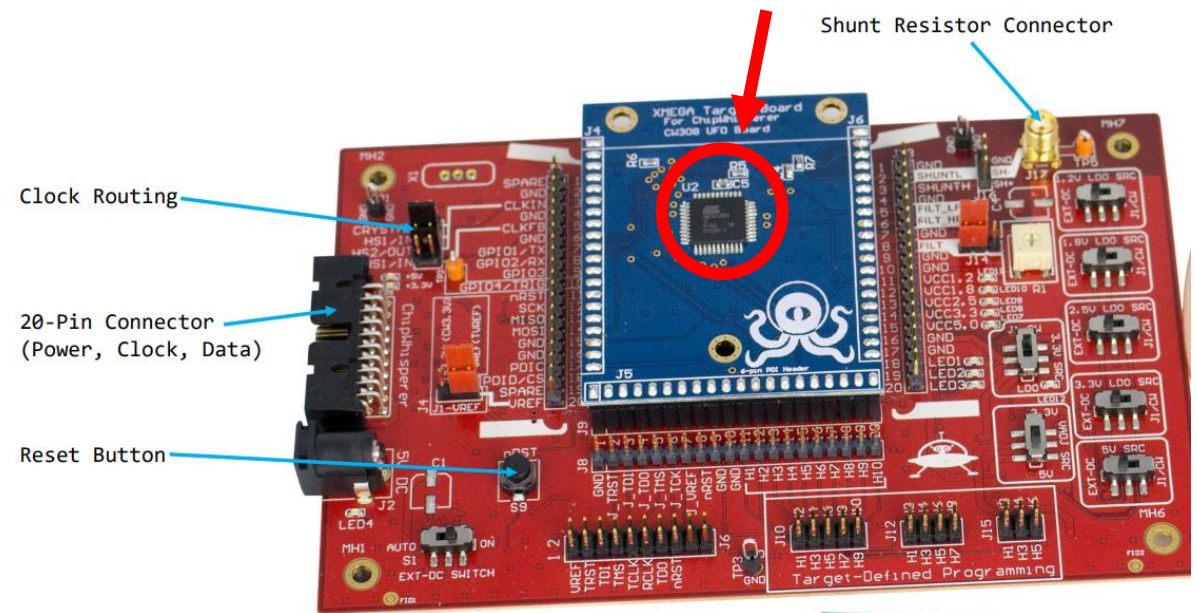
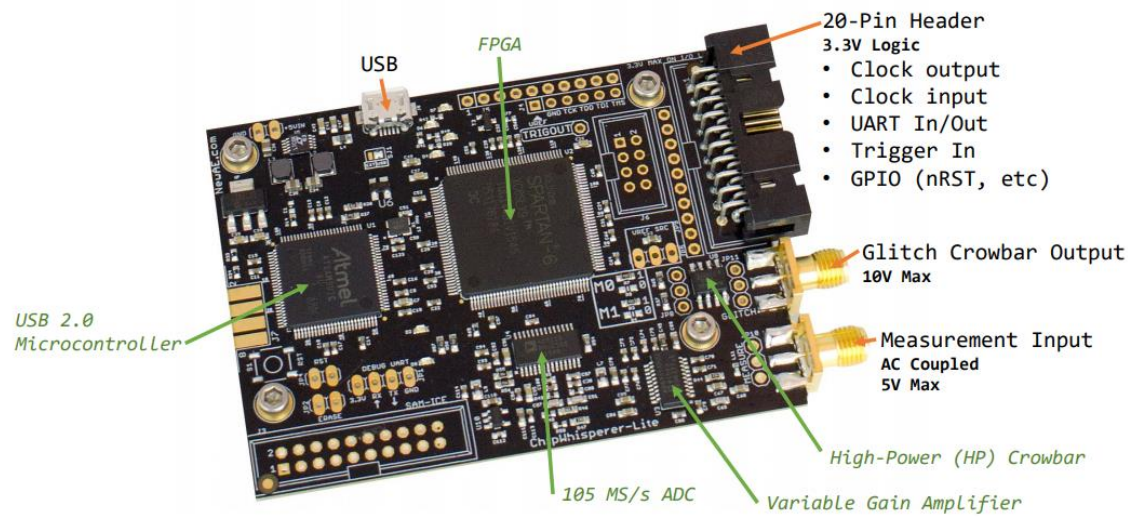
LAB

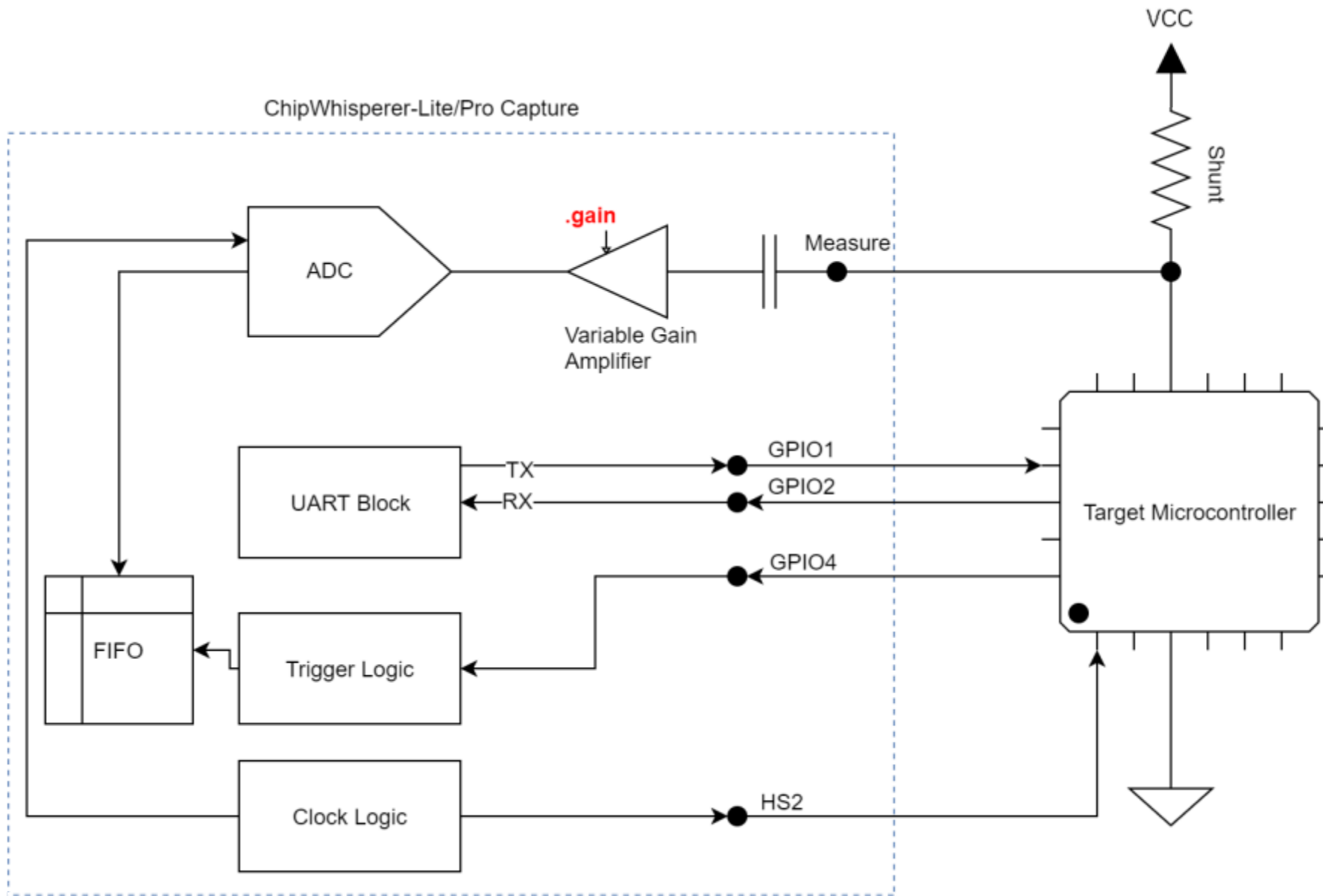
- Chipwhisperer
- Sinyal Analizi
- Zamanlama Saldırısı
- Basit Güç Analizi


Chipwhisperer



<https://www.newae.com/chipwhisperer>


















 Branch: develop ▾

Go to file


Add file ▾

 Clone ▾

	...	 3,676 commits	 7 branches	 40 tags
 docs	Docs updates - add glitch_lp docs (whoops!)	yesterday		
 hardware	Make simpleserial glitch password input 5 chars instead of 8	2 days ago		
 jupyter @ 7ee8e52	Update jupyter	last month		
 openadc @ 9bebfcb	FPGA: Add trigger out to CW-Lite (on by default now)	2 years ago		
 software	Docs updates - add glitch_lp docs (whoops!)	yesterday		
 tests	Add test for using short segments	2 months ago		
 tutorials @ 1f79b63	Update tutorials reference	11 months ago		
 .gitignore	Add swap files to gitignore	4 months ago		
 gitmodules	Add tutorials as submodule	12 months ago		

About


ChipWhisperer - the complete open-source toolchain for side-channel power analysis and glitching attacks


 chipwhisperer.com

security


side-channel

chipwhisperer

 Readme

 View license

Releases 40

 ChipWhisperer 5.2.1

Latest

on 27 May

LAB – 1

- SİNYAL ANALİZİ

LAB çalışmalarında kullanılan Jupyter Notebook dosyalarına aşağıdaki linkten erişebilirsiniz:

<https://github.com/mustafasirinn/Donanim-Guvenligi-Egitimi>

LAB – 2

- ZAMANLAMA SALDIRISI

LAB çalışmalarında kullanılan Jupyter Notebook dosyalarına aşağıdaki linkten erişebilirsiniz:

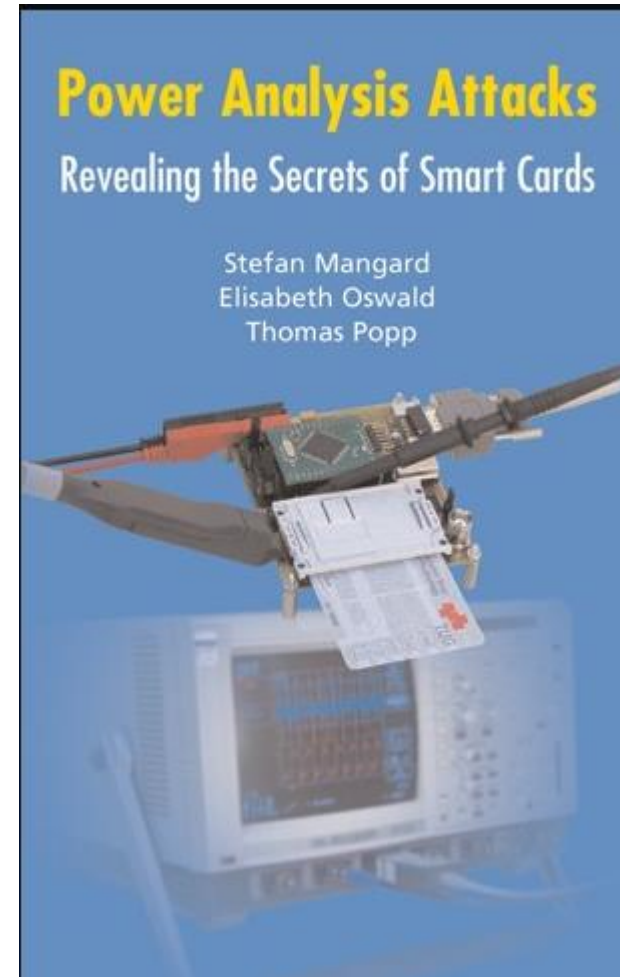
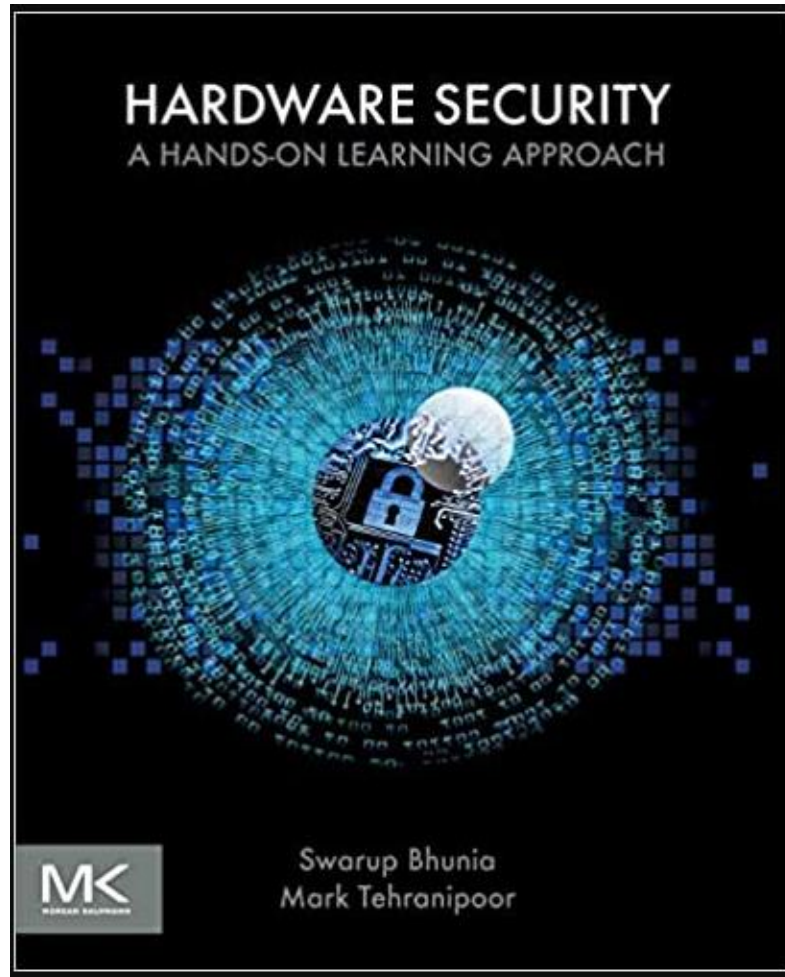
<https://github.com/mustafasirinn/Donanim-Guvenligi-Egitimi>

LAB – 3

- BASİT GÜÇ ANALİZİ SALDIRISI

LAB çalışmalarında kullanılan Jupyter Notebook dosyalarına aşağıdaki linkten erişebilirsiniz:

<https://github.com/mustafasirinn/Donanim-Guvenligi-Egitimi>



Teşekkürler..

Mustafa ŞİRİN

mustafa.sirin@istanbul.edu.tr